MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

DOMANDA DI INVENZIONE NUMERO	**102015000085038**
Data Deposito	**18/12/2015**
Data Pubblicazione	**18/06/2017**

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	21	10

Titolo

METODO DI PROTEZIONE DI FILE MULTIMEDIALI DA COPIA E DISTRIBUZIONE NON AUTORIZZATA E FILE MULTIMEDIALE ASSOCIATO.

Descrizione dell'invenzione avente per titolo:

"METODO DI PROTEZIONE DI FILE MULTIMEDIALI DA COPIA E DISTRIBUZIONE NON AUTORIZZATA E FILE MULTIMEDIALE ASSOCIATO"

a nome: PRB S.r.l.

a: Milano (MI)

Inventori: CARBONERA Antonio; FORLANI Paolo; GARAVAGLIA Roberto

---

Campo dell'invenzione

La presente invenzione riguarda il campo dei file multimediali ed in dettaglio comprende un metodo per impedire la copia e la distribuzione non autorizzata dei file multimediali.

Tecnica Nota

Allo stato attuale, quasi la totalità dei contenuti multimediali è di tipo digitale. La digitalizzazione comporta grandi vantaggi, quali ad esempio la possibilità di copia senza alcuna perdita di qualità, la possibilità di distribuzione per mezzo di reti quali Internet, la durata pressoché illimitata dei supporti.

Purtroppo però proprio uno dei vantaggi principali che è la possibilità di copiare il file digitale che contiene il dato multimediale, rappresenta un grosso inconveniente quando il contenuto è soggetto a diritti d'autore; la copia e la distribuzione illecita dei file multimediali, anche se vietate, sono molto diffuse e provocano un grandissimo danno agli autori e a tutti gli operatori della catena distributiva.

Il documento RM2013A000728 descrive un metodo per scambiare dati e comandi tra un computer e una periferica per mezzo di un file condiviso.

Il documento 102015000043174 prevede la possibilità di allocare il file nel computer o nel cloud anziché nella periferica come indicato nella figura 1. In tale documento, e con riferimento alla figura 2, è indicato nel suo complesso un

sistema real time di memorizzazione e trasmissione bidirezionale dei comandi e dei dati per un elaboratore elettronico nel processo di I/O.

Tra l'elaboratore 21 e la periferica 23 sussiste una connessione diretta USB 22, realizzata in dettaglio tra il computer host 21 e la periferica 23, sempre tramite USB o altro protocollo di comunicazione.

Nella forma di realizzazione descritta nella presente invenzione il file di comunicazione 24 è nel computer 21 e non nella periferica 23.

Questa disposizione può essere realizzata, ad esempio, sfruttando il protocollo USB OTG prima descritto. Preferibilmente ma non limitatamente, in questo caso, la periferica 23 deve disporre della completa funzionalità di master MSD (Mass Storage Device) che nel brevetto originale non era necessaria.

La configurazione qui descritta presenta alcuni vantaggi. Il primo vantaggio consiste nel fatto che il file di comunicazione, realizzato all'interno del disco del computer 21 o sotto forma di "ram disk", può avere dimensioni di gran lunga maggiori di quelle realizzabili all'interno della periferica 23. Nel caso in cui i dati sono trasmessi secondo la tecnica FIFO descritta nel brevetto RM2013A000728, si può aumentare a piacimento la quantità dei dati che possono restare in sospeso.

Un secondo vantaggio è dato dal fatto che un disco realizzato nel computer è molto più veloce di quello che può essere realizzato nella memoria RAM della periferica; questo vale in particolare in caso di "ram disk".

Un terzo vantaggio, disponibile se il disco è realizzato nel disco non volatile del computer 21 (magnetico o flash), è la "non volatilità" dei dati e dei comandi. Se la periferica si spegne o viene scollegata, ed anche se il computer viene spento e riacceso, il contenuto del file di comandi resta disponibile e le funzioni interrotte possono essere riprese esattamente dal momento dell'interruzione.

Un ulteriore vantaggio è quello di eliminare il problema che si presenta, in particolare con le unità viste come "disco di rete" come sopra descritto. Essendo

il file all'interno del computer stesso, anche in un computer virtualizzato (come ad esempio in un "thin client") il file può essere aggiornato immediatamente sfruttando le funzioni di lettura/scrittura non bufferizzate su disco fisico.

In figura 3 è mostrata una seconda forma di realizzazione del sistema real time di memorizzazione e trasmissione bidirezionale dei comandi e dei dati per un elaboratore nel processo di I/O oggetto della presente invenzione. In tale seconda forma di realizzazione, il file 34 è condiviso simultaneamente con più di una periferica 33 per mezzo di più connessioni 32. In tal modo è possibile trasmettere gli stessi dati a più periferiche 33 contemporaneamente senza doverli replicare. Ognuna delle periferiche 33 collegate può avere una propria area di comandi separata da quella delle altre periferiche collegate allo stesso file, e in tal caso la coda FIFO può funzionare esattamente come nel caso del brevetto RM2013A000728; oppure la trasmissione può avvenire in "streaming", senza aggiornamento dei puntatori da parte delle periferiche che ricevono i dati. In tal caso la trasmissione, similmente a un broadcast UDP, non ha un controllo di flusso.

Nel caso di condivisione di file tra due o più periferiche, è anche possibile che due periferiche si scambino tra di loro dati e comandi, senza intervento da parte di programmi presenti nel computer host, oppure che i dati originati da una periferica siano ricevuti dal computer e allo stesso tempo da altre periferiche.

Tornando alla figura 2 attraverso il posizionamento del file 24 di comandi e dati entro l'elaboratore 21 e comunque fuori dalla periferica si può fare operare il sistema oggetto della presente invenzione mediante funzionamento disconnesso. Si sfrutta la possibilità di realizzare all'interno del file di comunicazione delle code FIFO di dati e di comandi.

Se si tiene disconnessa la periferica durante una sessione di trasferimento di dati e comandi (si pensi ad esempio ad un'operazione di stampa tradizionale o di stampa 3D), i dati e i comandi che non sono scaricati dalla periferica si

accumulano all'interno del file. Quando, a sessione terminata, la periferica viene ricollegata, essa scarica comandi e dati dalle code nel file e la sessione viene eseguita esattamente come se la periferica 23 fosse stata sempre collegata. Si può anche trasferire o copiare il file accumulato durante la sessione in un altro computer e collegare a questo la periferica, ottenendo l'effettuazione della sessione ("playback") in un luogo diverso.

Nel caso, ad esempio, di un'operazione lunga quale una stampa 3D, è possibile preparare un file di "sessione di stampa" in un computer 21 dotato della potenza di elaborazione necessaria, per poi trasferire il file ed eseguire la stampa con un secondo computer non dotato di alcuna capacità di elaborazione grafica. Un altro vantaggio è dato dal fatto che il file trasferito (anche in più copie) non è il file grafico 3D, ma un file 24 di comandi e dati di cui si può solo effettuare il playback e dal quale non si può risalire al file originale. Il file grafico infatti potrebbe essere soggetto a diritti di proprietà e riservatezza che ne renderebbero problematico il trasferimento. Sempre per tutelare i diritti, per mezzo di adatte tecniche crittografiche è anche possibile limitare il numero di esecuzioni del playback del comando e stabilire dei limiti temporali alla sua esecuzione.

In definitiva, questa applicazione della tecnologia permette la "virtualizzazione", anche controllata, di una sessione di lavoro.

Una terza forma di realizzazione è descritta in figura 4. In tale terza forma di realizzazione del sistema oggetto della presente invenzione, il file di comunicazione 44 è vantaggiosamente allocato in un server remoto o, secondo la denominazione attualmente più diffusa, è "in cloud".

Il file 44 è sempre condiviso tra computer 41 ed una o più periferiche 43, che vi accedono tramite commessioni Internet schematizzate nella figura con il numero 42.

Anche in questo caso computer 41 e periferica 43 si possono scambiare dati e comandi esattamente come nel brevetto originale RM2013A000728.

La minore velocità e stabilità di questo genere di connessione sono ampiamente compensate dalla possibilità di operare comunque, qualsiasi sia la distanza tra il computer e la periferica.

Una quarta forma di realizzazione del sistema oggetto della presente invenzione è infine descritta in figura 5. In tale quarta forma di realizzazione si utilizza un programma applicativo "in cloud" detto anche "SaaS", nell'esempio un gestore di spreadsheet quale ad esempio "Fogli Google". Due computer 51 e 53 sono collegati tramite Internet 52 al programma applicativo in cloud, che presenta ad ambedue i computer lo spreadsheet 54. Invece di settori del disco o di byte all'interno dei settori, in questo caso i dati, i comandi e le risposte sono posizionati in celle del foglio identificate da numero di riga e lettera di colonna. Sequenze di dati, anziché in settori del disco come nel brevetto RM2013A000728, possono essere allocate in intere righe o colonne del foglio. Tutto il funzionamento dell'interfaccia è analogo a quello descritto nel brevetto RM2013A000728, permettendo così lo scambio di dati e comandi tra i due computer. Se occorre agire su periferiche come la 56, queste possono essere collegate ad uno dei due computer con un'interfaccia 55 che può essere sia di tipo tradizionale, sia del tipo secondo il brevetto RM2013A000728, in questo caso operante su un apposito file di dati e comandi.

Nei due computer 51 e 53, un apposito programma applicativo provvede alla comunicazione con l'applicazione "Fogli Google" per mezzo dell'API (Application Program Interface) prevista dal fornitore del servizio in cloud. Quindi non c'è alcuna necessità di rendere il foglio leggibile ad un operatore umano e nemmeno di renderlo visibile agli utenti. La diagnostica e la messa a punto possono comunque essere effettuate osservando lo spreadsheet, eventualmente aprendolo in un terzo computer.

Mentre l'esempio sopra riportato usa un gestore di spreadsheet per la comunicazione di dati e comandi, è anche possibile usare altri tipi di programmi

applicativi in cloud, quale ad esempio un editore di testi; in tal caso dati e comandi sono posizionati in locazioni predefinite di un documento di testo.

In definitiva, mentre il brevetto RM2013A000728 prevede l'allocazione nella periferica del file usato per la comunicazione di dati e comandi, il trovato qui descritto aggiunge la possibilità di allocarlo vantaggiosamente nel computer host oppure nel cloud.

Nel documento 102015000043174, la richiedente tendeva a precisare che il programma applicativo che viene eseguito nel computer host e che realizza la funzionalità generale del sistema computer-periferica non deve essere modificato in seguito alla diversa allocazione del file, perché al fine del programma cambia solo la cartella logica in cui il file deve essere aperto.

Si può anche concepire un programma che, quando avviato, effettua una "ricerca per nome" del file di comunicazione in tutte le cartelle disponibili nel computer, eliminando quindi anche la necessità di definire la cartella in una fase di configurazione iniziale.

Nella descrizione si è fatto riferimento in più punti all'uso dello standard USB per la comunicazione; è comunque chiaro che la comunicazione può avvenire con qualsiasi standard attuale (es. SCSI, SAS, SATA, FireWire..) ed ulteriori standard futuri senza per questo uscire dall'ambito di protezione del brevetto.

In ognuno dei tre casi principali e anche nel caso secondario di uso di spreadsheet in cloud, il metodo presenta numerosi vantaggi, tra i quali la possibilità di realizzare un'interazione tra un computer e una o più periferiche senza usare driver, semplificando i programmi applicativi e permettendo un'interazione a qualsiasi distanza a basso costo.

Il documento RM2013A000728 e parte della presente descrizione fanno riferimento all'uso della tecnica per l'interfacciamento di una tavoletta digitalizzatrice, ma è chiaro che la stessa tecnica può essere vantaggiosamente

usata in ogni caso in cui un elaboratore comunica con una o più periferiche.

Infine il brevetto 102015000056882 estende le funzionalità del brevetto originale aggiungendo caratteristiche di sicurezza e di protezione dei dati.
In tale documento, viene descritto un metodo di scambio di dati e comandi sicurizzato, tra due dispositivi uno ricevente ed uno trasmittente che sono visti, in particolare per quanto riguarda una periferica, come una memoria di massa e dunque possono operare con uno scambio di dati e comandi in modalità driverless.

Come si è detto, conoscendo la tecnica di scambio dati e comandi tramite file descritta nel brevetto RM2013A000728 è possibile, con uno sforzo limitato, leggere i dati trasmessi. Infatti, anche non conoscendo le reali posizioni dei byte di controllo (ad esempio quelli che contengono i puntatori ai settori in lettura e scrittura) e le reali posizioni dei settori in cui sono allocati i dati da scambiare, è possibile ricavare tali posizioni per mezzo di un'attenta osservazione, eventualmente automatizzata, dei dati e settori interessati ad uno scambio.

Infatti i settori che contengono i byte di controllo della trasmissione (i puntatori) sono letti e scritti ad ogni operazione di lettura e scrittura dei settori di dati, quindi ad un settore di questo tipo si fa accesso molto più frequentemente che a quelli che contengono i dati: è quindi possibile capire quali sono i settori relativi ai byte di controllo.

Un successivo esame del contenuto dei byte all'interno di un settore di controllo permette di individuare quali sono i puntatori, perché essi si incrementano regolarmente fino a puntare all'ultimo settore di dati e poi tornano indietro a puntare al primo settore di dati e riprendono quindi ad incrementarsi. I settori di dati sono anch'essi facilmente riconoscibili perché vi si accede sequenzialmente, uno dopo l'altro, prima in scrittura e poi in lettura. Quindi si può affermare che, per mezzo dell'analisi di una certa quantità di dati trasmessi, è possibile ricavare l'organizzazione dei dati nel disco di scambio e quindi è

possibile estrarre tutti i dati scambiati in seguito con lo stesso protocollo.

La tecnica che è oggetto della invenzione secondo il documento 102015000056882 si basa sul fatto che la decodifica dei dati scambiati è di gran lunga più difficile se la posizione dei dati all'interno del file di scambio cambia frequentemente, ad esempio ad ogni nuovo scambio di dati.

Con riferimento alla figura 6, è indicata l'organizzazione logica dei settori del file 100 di scambio dati e comandi (che per semplicità è rappresentato come formato da soli 8 settori). Il primo settore, indicato con 0 e tratteggiato, è quello che contiene i byte di controllo della comunicazione (byte di stato e puntatori). Ognuno dei settori dei file è, secondo il presente metodo, in realtà allocato nel disco in una diversa posizione: il settore 0 è allocato nel settore fisico 3, il settore 1 nel 6 e così via. Per stabilire la posizione dei settori si usa un "algoritmo di scrambling" 200, che è un procedimento matematico che, a partire da un insieme finito di numeri interi, genera un secondo insieme o file 101 formato dagli stessi numeri, ma scambiati tra loro secondo una legge apparentemente casuale.

Con riferimento alla figura 7, la quale illustra il detto algoritmo di scrambling, si vede che i numeri interi appartenenti ad un insieme ordinato di A, per mezzo della trasformazione C, detta scrambling 200, sono collegati ad altrettanti numeri interi del secondo insieme B in modo apparentemente casuale. In realtà l'algoritmo di scrambling si basa su una chiave di scrambling D, che è un grande numero intero e opera in modo tale che la stessa chiave, applicata in momenti o luoghi diversi, produce sempre la stessa corrispondenza tra i due insiemi di numeri.

Quindi, analogamente ad un algoritmo di crittografia, il possesso della chiave di scrambling D permette a due soggetti di costruire la stessa corrispondenza. Detta chiave di scrambling è mantenuta segreta.

Nella tecnica oggetto del presente brevetto, la chiave di scrambling viene scambiata, per ogni nuovo trasferimento di dati, con l'algoritmo Diffie-Hellman

secondo la tecnica già descritta nel brevetto RM2013A000728, quindi l'allocazione dei settori del disco cambia con legge apparentemente casuale ad ogni nuova comunicazione tra il computer e la periferica e/o viceversa.

Un ulteriore livello di sicurezza può essere ottenuto per mezzo dello scrambling applicato, all'interno di ogni settore, all'allocazione dei singoli byte che lo compongono. La chiave usata può essere la stessa usata per lo scrambling dei settori oppure una seconda chiave anch'essa concordata in anticipo tramite Diffie-Hellman.

La Richiedente fa notare che, usando la tecnica qui descritta, è anche possibile usare contemporaneamente la cifratura a blocchi dei dati contenuti nei settori, con un algoritmo simmetrico "tradizionale" quali ad esempio DES, 3DES o AES.

Il vantaggio della protezione per mezzo dello scrambling è duplice: prima di tutto, non permette a chi intercetta la comunicazione di leggere i byte di controllo della comunicazione e quindi di seguirne (o eventualmente modificarne) l'andamento; in secondo luogo lo scrambling è meno oneroso dal punto di vista computazionale rispetto ad un algoritmo crittografico tradizionale, quindi è più facilmente realizzabile nel caso di periferiche dotate di piccoli microcontrollori con limitate capacità di elaborazione.

Viceversa, nel caso in cui si desideri la massima sicurezza possibile, è possibile usare la tecnica di scrambling, ma cifrando anche i blocchi di dati con un algoritmo simmetrico tradizionale. La chiave di cifratura simmetrica può essere una seconda o terza chiave scambiata sempre all'inizio di ogni nuova comunicazione.

Sia nel caso di uso dello scrambling da solo, sia nel caso di uso congiunto scrambling+cifratura simmetrica, le chiavi possono essere scambiate con qualsiasi periodicità, secondo il livello di sicurezza desiderato: solo una volta; ad ogni nuova sessione; ad ogni nuovo scambio di dati; periodicamente anche

all'interno dello stesso scambio di dati.

Tutti i metodi finora descritti si basano su uno scambio, più o meno frequente, di chiavi segrete e condivise per mezzo del noto metodo Diffie-Hellman ma, come scritto sopra, tale metodo non è utilizzabile nel caso in cui il computer e la periferica non sono connessi tra loro e il file di scambio dati e comandi è usato per accumulare una sessione di lavoro da effettuare in diversi tempi e luoghi.

Nel caso del funzionamento disconnesso si usa una tecnica addizionale descritta nel seguito.

Il destinatario di un file di scambio dati e comandi (persona fisica, organizzazione oppure macchina periferica, ad esempio stampante 3D), viene preventivamente dotato di una coppia di chiavi di cifratura asimmetrica, ad esempio secondo il metodo RSA. La chiave privata resta segreta all'interno della periferica mentre quella pubblica è inviata al mittente (persona fisica, organizzazione oppure computer) con qualsiasi mezzo a disposizione, ad esempio tramite Internet oppure con l'invio di un file su mezzo fisico.

Come indicato in figura 8, il dispositivo che genera il file di scambio dati e comandi 100 (computer mittente) genera, per mezzo di un generatore di numeri casuali, le chiavi segrete 300. Le chiavi segrete 300 sono: l'eventuale chiave di crittografia simmetrica K1 usata per cifrare i dati (con algoritmo DES, 3DES, AES o simili); la chiave di scrambling dei settori K2; l'eventuale chiave di scrambling dei byte all'interno dei settori K3. Il numero di chiavi segrete 300 qui descritto come tre non è da considerarsi limitativo al fine dell'ambito di protezione fornito dalle rivendicazioni.

Il computer mittente provvede quindi, per mezzo del codificatore RSA 402, a cifrare le chiavi segrete 300 con la chiave pubblica 400 del destinatario. Il codificatore RSA 402 presenta dunque un primo ed un secondo ingresso 402', 402'' rispettivamente alimentati con le chiavi segrete 300 e con la chiave

pubblica 400, e produce il messaggio codificato sulla sua uscita 403. Il risultato prodotto sull'uscita 403 del codificatore RSA 402, cioè l'insieme delle chiavi segrete 300, viene scritto in uno dei settori del file di scambio 100, indicato con E nella figura 3. Il settore E è allocato in una posizione predeterminata; se la lunghezza delle chiavi è tale da richiedere più di un settore, è allocato un numero sufficiente di settori contigui o separati 404. Eventualmente la detta posizione predeterminata è generata a sua volta da un generatore di numeri casuali, e il numero corrispondente al detto settore E viene condiviso tra computer e periferica. In questo modo la sicurezza della trasmissione viene aumentata di volta in volta. Il file così protetto viene memorizzato ed inviato alla periferica che lo dovrà attuare.

Con riferimento alla figura 9, la periferica, allorquando ha ricevuto il file 100 di scambio di dati e comandi, dapprima estrae dal file di scambio le chiavi segrete E dal detto file 100 e per mezzo di un decodificatore RSA 502 provvede a decifrare le chiavi usando la propria chiave privata 500. Analogamente al caso del codificatore, il decodificatore RSA comprende un primo ed un secondo ingresso 502', 502'' alimentati rispettivamente dalle chiavi E e dalla chiave privata 500 e produce in uscita le chiavi decodificate K1-K3 600.

A questo punto sono disponibili le chiavi segrete K1-K3 per la decifratura e per il "descrambling" dei dati e il processo di esecuzione dei comandi contenuti nel file e di estrazione dei dati avviene come prima descritto per il caso in cui le chiavi sono scambiate con l'algoritmo Diffie-Hellman.

Veduto quanto sopra, lo scopo della presente invenzione è dunque quello di descriver un metodo per impedire la copia e la distribuzione non autorizzata dei file multimediali.

Sommario dell'invenzione

Secondo la presente invenzione viene realizzato un metodo di protezione di file multimediali da copia e distribuzione non autorizzata, il detto metodo

essendo caratterizzato dal fatto di comprendere:

- un passo di creazione di un file multimediale in una memoria, in cui il detto file multimediale presenta una pluralità di settori;
- un passo di creazione su detto file multimediale di un settore d'autorizzazione, in cui in detto settore d'autorizzazione vengono memorizzati una pluralità di permessi di accesso e/o lettura del detto file multimediale;
- un passo di creazione in detta memoria di una tavola di allocazione di una pluralità di settori di dati e comandi di detto file multimediale;
- un passo di crittazione del detto settore d'autorizzazione e della detta tavola di allocazione di una pluralità di settori di dati e comandi di detto file multimediale, in cui la crittazione avviene con una prima chiave di crittazione pubblica.

In un aspetto della presente invenzione, in detto metodo, in un passo di scaricamento del detto file multimediale il detto file multimediale viene scaricato un settore per volta in un file di destinazione contenuto in una memoria di destinazione, ed in cui è presente un passo di lettura ripetuto per ogni settore scaricato, in cui un programma per elaboratore accede al sistema operativo o ad una tabella di allocazione dei file della detta memoria di destinazione, e carica un indirizzo fisico del settore appena scaricato.

In un aspetto della presente invenzione, in detto metodo, il detto programma per elaboratore, dopo aver acceduto al detto sistema operativo o alla detta tabella di allocazione di file, aggiunge una nuova riga ad una tabella di allocazione dei settori di dati e comandi e ripete i passi di trasferimento di ricavo dell'indirizzo fisico e di scrittura di una nuova riga fino alla fine del detto file multimediale.

In un aspetto della presente invenzione, in detto metodo, il detto programma per elaboratore esegue una generazione di detto settore d'autorizzazione ed esegue un passo di memorizzazione entro il detto settore d'autorizzazione di permessi di utilizzo del file.

In un aspetto della presente invenzione, in detto metodo, il detto programma

per elaboratore, al termine del detto passo di memorizzazione esegue un passo di codifica della tavola di allocazione dei settori di dati e comandi sul detto file di destinazione e chiude il detto file.

In un aspetto della presente invenzione, in detto metodo, è presente un passo di riproduzione del detto file multimediale in cui si ha dapprima un passo di lettura della tavola di allocazione dei settori di dati e comandi e un successivo passo di decrittazione della detta tavola di allocazione dei settori di dati e comandi del detto file multimediale.

In un aspetto della presente invenzione, in detto metodo, il detto passo di decrittazione avviene impiegando la detta prima chiave di crittazione pubblica.

In un aspetto della presente invenzione, in detto metodo, sono presenti un passo di decrittazione del detto settore d'autorizzazione e un passo di caricamento di una pluralità di dati di autorizzazione contenuti nel detto settore d'autorizzazione dopo la decrittazione.

In un aspetto della presente invenzione, in detto metodo, una riproduzione elettronica del detto file multimediale avviene solamente allorquando i detti dati di autorizzazione comprendono un'autorizzazione alla detta riproduzione.

In un aspetto della presente invenzione, in detto metodo, nella riproduzione del detto file multimediale si ha una lettura sequenziale della pluralità di settori del detto file multimediale impiegando la detta tavola di allocazione dei settori di dati e comandi memorizzata nel file multimediale stesso.

In un aspetto della presente invenzione, in detto metodo, è presente un passo di caricamento di almeno parte della detta pluralità di settori del detto file multimediale in uno stadio buffer di un dispositivo elettronico di riproduzione del detto file.

In un aspetto della presente invenzione, in detto metodo, all'interno di almeno parte dei detti settori del detto file multimediale sono contenuti dati utili cifrati mediante codifica simmetrica con una chiave di scrambling.

In un aspetto della presente invenzione, in detto metodo, la detta chiave di scrambling è scritta nel detto file multimediale mediante codifica asimmetrica.

In un aspetto della presente invenzione, in detto metodo, la detta chiave di scrambling è una chiave ad uso singolo ottenuta da un sito internet predefinito.

In un aspetto della presente invenzione, in detto metodo, la detta chiave di scrambling è una chiave ad uso cablata all'interno di un programma per elaboratore di decodifica del detto file multimediale.

In un aspetto della presente invenzione, in detto metodo è presente un passo di copiatura del detto file multimediale a sua volta comprendente un passo di decodifica della detta tavola di allocazione di settori di dati e comandi e del detto settore d'autorizzazione del detto file multimediale ed un successivo passo di lettura da detta tavola di allocazione di settori di dati e comandi del detto file multimediale di un settore ed un passo di successiva scrittura del settore appena letto in un file di destinazione.

In un aspetto della presente invenzione, in detto metodo a seguito del detto passo di successiva scrittura del settore appena letto in detto file di destinazione, il detto programma per elaboratore legge il numero fisico del settore del file di destinazione appena scritto e aggiunge una riga contenente tale numero fisico nella tavola di allocazione dei settori di dati e comandi del detto file di destinazione.

Secondo la presente invenzione viene realizzato un programma per elaboratore elettronico, caricato su di un supporto di memoria non transitorio e atto ad essere eseguito su di un elaboratore elettronico, il detto programma essendo atto causare l'esecuzione di almeno parte dei passi descritti in una qualsiasi dei passi descritti precedentemente.

Secondo la presente invenzione viene inoltre realizzato un file multimediale caratterizzato dal fatto di comprendere una struttura avente una pluralità di settori, in cui in detta pluralità di settori, almeno parte è atta a contenere dati utili

multimediali ed in cui in detta pluralità di settori sono presenti:

- almeno un settore d'autorizzazione contenente dati elettronici di autorizzazione alla lettura o copiatura dei detti dati utili multimediali e/o del detto file multimediale stesso; e
- una tavola di allocazione di settori di dati e comandi del detto file multimediale in cui la detta tavola di allocazione di settori di dati e comandi del detto file multimediale è crittata assieme al detto settore d'autorizzazione.

Descrizione delle figure

L'invenzione verrà ora descritta facendo riferimento alle figure annesse nelle quali:

- la figura 1 illustra un sistema real time di memorizzazione e trasmissione bidirezionale dei comandi e dei dati per un elaboratore nel processo di I/O in una sua forma di realizzazione nota dal documento RM2013A000728;
- la figura 2 illustra un sistema real time di memorizzazione e trasmissione bidirezionale dei comandi e dei dati per un elaboratore nel processo di I/O in una sua prima forma di realizzazione nota;
- la figura 3 illustra un sistema real time di memorizzazione e trasmissione bidirezionale dei comandi e dei dati per un elaboratore nel processo di I/O in una sua seconda forma di realizzazione nota;
- la figura 4 illustra un sistema real time di memorizzazione e trasmissione bidirezionale dei comandi e dei dati per un elaboratore nel processo di I/O in una sua terza forma di realizzazione nota;
- la figura 5 illustra un sistema real time di memorizzazione e trasmissione bidirezionale dei comandi e dei dati per un elaboratore nel processo di I/O in una sua quarta forma di realizzazione nota;
- la figura 6 illustra una pluralità di file con settori scambiati e ordine di scambio;
- la figura 7 illustra un ordine di scambio dei settori dei detti file;

- la figura 8 illustra un diagramma di codifica di un file;
- la figura 9 illustra un diagramma di decodifica di un file; e per quanto riguarda specificamente l'oggetto della presente invenzione;
- la figura 10 illustra una memoria di massa ove è presente una struttura di file multimediale;
- la figura 11 illustra un diagramma di flusso di un processo di scaricamento del detto file multimediale oggetto della presente invenzione;
- la figura 12 illustra un diagramma di flusso di un processo di riproduzione di un file multimediale oggetto della presente invenzione; e
- la figura 13 illustra un digramma di flusso di un processo di copia di un file multimediale oggetto della presente invenzione.

Descrizione dettagliata dell'invenzione

Un file di scambio dati e comandi secondo il brevetto RM2013A000728 prevede una allocazione strettamente consecutiva dei settori del disco che contengono il file.

Questa caratteristica, realizzata in una periferica governata da un microcontrollore, presenta il vantaggio di una semplificazione nell'accesso al file da parte del microcontrollore.

Se invece si desidera usare un file formato secondo i brevetti citati per contenere dati multimediali, la maggior potenza di elaborazione del processore multimediale che elabora i dati rende non più necessaria l'allocazione consecutiva e il file, che può risiedere in un computer, in un tablet o smartphone o in un riproduttore multimediale, può essere allocato secondo qualsiasi sequenza e, in particolare nei sistemi FAT che sono i più diffusi nei supporti portatili quali "chiavette USB" e schede di memoria SD e similari, potrà avere qualsiasi grado di frammentazione.

Ai sensi della presente invenzione si ricorda che per "frammentazione" si intende la allocazione di un file in settori non consecutivi, ma distanti tra loro e

"sparpagliati" nel disco e comunque non uno consecutivo all'altro. La frammentazione normalmente rappresenta un inconveniente, perché rallenta gli accessi in lettura e scrittura al file, ma nella presente invenzione viene sfruttata per proteggere un file dalla copia non autorizzata.

La figura 10 illustra un file multimediale introdotto in una memoria di massa 1000. Un file multimediale 1002 realizzato secondo la presente invenzione contiene, in una posizione predeterminata (ad esempio alla fine), una mappa dei settori fisici in cui il file stesso è allocato, cifrata con algoritmo asimmetrico usando come chiave una chiave pubblica del destinatario autorizzato all'utilizzo dei dati multimediali.

Il file multimediale 1002 contiene poi i dati multimediali, organizzati in forma di coda di dati e protetti contro la copia non autorizzata usando il metodo descritto nel documento IT102015000056882.

Il file multimediale 1002 contiene anche, sempre cifrato con la stessa chiave, un settore P, indicato con il numero di riferimento 1004, in cui sono contenuti i permessi relativi al file: l'autorizzazione alla copia ed eventualmente il numero di copie permesse; un eventuale numero massimo di riproduzioni permesse; una eventuale data di scadenza delle autorizzazioni.

Il file multimediale 1002 così strutturato non può essere usato tale e quale, ad esempio usando i normali programmi di riproduzione quale ad esempio Windows Media Player con un codec standard, ma deve essere riprodotto con un programma o un codec specificatamente concepito, in grado di decodificarlo correttamente. Anche la copia, se permessa, non può essere realizzata per mezzo delle normali funzioni del sistema operativo ma per mezzo di un programma apposito. Infatti la normale copia, pur sempre possibile, effettuata per mezzo del sistema operativo, produce un file che non può più essere riprodotto nemmeno usando il programma o il codec apposito sopra indicato.

Mentre non è possibile impedire la copia fatta per mezzo delle funzioni del

sistema operativo (ma che produce copie inutilizzabili), la tecnica qui descritta permette di impedire del tutto la copia in forma utilizzabile o di limitare il numero delle copie utilizzabili, ad esempio alle tre normalmente previste per l'uso personale.

Per potere usufruire di un file multimediale 1002 come quello oggetto della presente invenzione (ad esempio, musica o film), l'utente che lo acquisisce viene dotato di una coppia di chiavi di cifratura asimmetrica, la cui chiave privata gli viene consegnata in modo sicuro e che resta protetta all'interno del dispositivo riproduttore che intende usare (computer, tablet, smartphone o simile).

Per meglio descrivere la tecnica, occorre riferirsi alla figura 10, in cui si vede una rappresentazione schematica della memoria di massa 1000, organizzata a settori, in cui è memorizzato il file multimediale 1002.

Il file è formato di dati e comandi, indicati con il numero di riferimento 1005, organizzati secondo la tecnica descritta nel brevetto RM2013A000728 e contenenti i dati multimediali veri e propri; ma contiene anche ulteriori dati introdotti dal trovato qui descritto: un certo numero di settori, indicati con A, B.., che contengono una tavola di allocazione dei settori di dati e comandi indicata con il numero di riferimento 1003. Questa tavola di allocazione dei settori di dati e comandi indicata con 1003 è formata dalla serie (indicata con N1, N2... nella figura 10) degli indirizzi fisici dei settori che contengono i dati e i comandi del file.

Gli indirizzi fisici sono relativi alla numerazione reale dei settori in cui è suddiviso il disco, che, nel caso ad esempio del sistema FAT (che, essendo ben noto, non necessita di ulteriori spiegazioni), sono quelli riportati nella "file allocation table" del file stesso e possono essere ricavati da funzioni di basso livello del sistema operativo. Pertanto, la tavola di allocazione dei settori è un sottoinsieme della file allocation table del file multimediale 1002 stesso.

La tavola di allocazione dei settori di dati e comandi indicata con 1003,

anche se per semplicità appare in chiaro nella figura 10, è in realtà cifrata assieme al settore P (indicato con il numero di riferimento 1004) usando la chiave pubblica di crittografia asimmetrica associata all'utente autorizzato alla riproduzione.

Nel seguito della presente descrizione sono spiegati i dettagli operativi delle tre fasi che tipicamente compongono la vita di un file multimediale: lo scaricamento da Internet, la riproduzione e la copia.

Nella seguente porzione di descrizione viene descritto lo scaricamento di un file multimediale; tale descrizione fa riferimento al diagramma di flusso rappresentato a supporto della descrizione in figura 11.

Lo scaricamento da Internet si può fare per mezzo di un programma per elaboratore elettronico, di una applicazione software, oppure di un oggetto attivo incorporato in una pagina Web e richiede che tale programma o applicazione possano accedere alle funzioni di basso livello del sistema operativo o comunque che possano leggere la "file allocation table" dell'unità di memoria di massa in cui il file multimediale viene scritto durante lo scaricamento.

Se il cedente del file ha deciso di non autorizzarne la copia, lo scaricamento può essere fatto solo direttamente nel dispositivo che sarà usato per la riproduzione, che in tal caso potrà essere anche a sola lettura (CD-ROM). Nei casi in cui è autorizzato un massimo numero di copie, è invece necessario che il supporto sia modificabile (hard disk, memoria Flash o simile).

Come si vede nella Figura 11, che rappresenta un diagramma di flusso semplificato di questa operazione, il file multimediale (già nel formato previsto dal brevetto RM2013A000728 e protetto come previsto nel brevetto 102015000056882) viene trasferito un settore per volta nel file di destinazione (passo 2100). Non appena il settore è stato scritto, il programma di scaricamento accede al sistema operativo o legge la FAT della memoria di massa per ricavare l'indirizzo fisico (numero di settore) in cui il settore è stato scritto (passo 2200);

il programma o la applicazione aggiunge quindi una riga alla propria tavola di allocazione dei settori di dati e comandi indicata con il numero di riferimento 1003 (passo 2300) e ripete il ciclo (passo 2400) fino alla fine del file.

Il programma quindi genera il settore P che contiene, in modo opportunamente codificato, i permessi di utilizzo del file (passo 2500), quindi codifica con la chiave pubblica dell'utente la tavola di allocazione dei settori di dati e comandi indicata con il numero di riferimento 1003 e il settore P (passo 2600). Infine scrive la tavola di allocazione dei settori di dati e comandi indicata con 1003 in posizione predeterminata nel file di destinazione (ad esempio alla fine) e chiude il file (passi 2700 e 2800).

Allorquando il file multimediale 1002 viene riprodotto, il metodo oggetto della presente invenzione opera come segue. In dettaglio, la descrizione dell'operazione del metodo oggetto della presente invenzione è coadiuvata dal supporto visuale fornito dal diagramma di flusso di figura 12.

La riproduzione (ad esempio di un file audio) può essere effettuata solo usando un programma apposito di riproduzione oppure installando, in un normale programma di riproduzione multimediale (quale ed esempio Windows Media Player), un codec plug-in realizzato per decodificare i file generati secondo la presente tecnologia. Con riferimento alla figura 12, la prima operazione (passo 3100) consiste nella lettura dal file della tavola di allocazione dei settori, che come si è detto è in una posizione predeterminata, e nella sua decodifica per mezzo della chiave privata dell'utente che effettua la riproduzione. Chiaramente un utente non autorizzato non dispone della chiave e non può effettuare la riproduzione.

Il settore P che contiene i permessi viene esaminato (fase 3200) per verificare se la riproduzione è permessa; la tecnologia permette infatti di stabilire un massimo numero di riproduzioni oppure un limite temporale di utilizzo del file.

A questo punto inizia il loop di lettura e riproduzione, formato dai passi 3300,3400,3500,3600. Ogni settore viene letto andandolo ad indirizzare per mezzo della tavola di allocazione settori letta dal file stesso (passo 3300), e non usando le funzioni del sistema operativo che permettono la lettura sequenziale del file. In questo modo, se il file è stato spostato o copiato, la riproduzione non può avvenire perché i settori in cui è scritto fisicamente il file non corrispondono più con quelli elencati nella tavola di allocazione letta dal file stesso.

I settori sono letti di seguito (passo 3400), eventualmente accumulati in un buffer di lettura e quindi riprodotti (passo 3500). Quando il file finisce, viene chiuso (passi 3600 e 3700).

Notare che, visto che l'allocazione reale dei settori del file è sempre ricavabile dal sistema operativo, sembra possibile che un programma di riproduzione scritto appositamente per aggirare la protezione possa decodificare il file. Questo non può avvenire perché, come si è detto, i dati e i comandi non sono comunque decodificabili, essendo per essi usata la tecnica descritta nel brevetto 102015000056882, che effettua uno "scrambling" ed una codifica simmetrica dei dati utili del file. Per realizzare il "descrambling" occorre disporre della chiave di scrambling che viene tenuta segreta: può essere fissa e cablata all'interno del programma di decodifica autorizzato, scritta nel file multimediale stesso in forma crittografata con algoritmo asimmetrico oppure ottenuta ogni volta da un servizio via rete Internet.

Se il file ha un massimo numero di riproduzioni autorizzate, deve necessariamente essere su supporto riscrivibile. In tal caso, il settore P viene aggiornato decrementando il numero di riproduzioni ancora permesse, viene nuovamente codificato con la chiave pubblica dell'utente e il settore del file che lo contiene viene riscritto al termine della riproduzione (o anche all'inizio della riproduzione, o dopo alcuni secondi, secondo la scelta del produttore).

La copia del file multimediale 1002, come si può vedere in figura 13, inizia

con la decodifica della tavola di allocazione settori e del settore P del file di origine (passo 4100). Se, come risulta dal settore P, la copia è permessa (passo 4200), si passa alla lettura del numero del settore da copiare dalla tavola di allocazione settori del file di origine (passo 4300); quindi avviene la lettura del settore dal file di origine (passo 4400), la scrittura del settore nel file di destinazione (passo 4500), la lettura del numero fisico del settore relativo al file di destinazione (passo 4600) a l'aggiunta di una riga contenente tale numero alla tavola di allocazione settori del file di destinazione (passo 4700).

La copia dei settori prosegue fino alla fine del file (passo 4800). Alla fine, viene creato un nuovo settore P per il file di destinazione, che contiene i diritti che il cedente del file ha stabilito: ad esempio, è possibile fare in modo che la copia sia riproducibile ma che non possa essere ulteriormente copiata (passo 4900). La nuova tavola di allocazione dei settori è quindi cifrata con la chiave pubblica del destinatario, che può essere lo stesso del file di origine oppure un altro (passo 5000), e quindi scritta nel file di destinazione nella posizione prestabilita (passo 5100). Il file è quindi chiuso (passo 5200).

Ulteriori metodi particolari vengono descritti nella presente parte della descrizione. Come si comprende dalla descrizione precedente, la protezione contro la copia è data dalla presenza della tavola di allocazione dei settori e dal fatto che, se quella presente nel file non coincide con quella in cui il file è realmente allocato, la riproduzione o la copia non sono possibili. Ne consegue che, ai fini della protezione, è preferibile che il file abbia un certo grado di frammentazione, perché una allocazione contigua dei settori è più facile da riprodurre. Esiste inoltre un caso particolare in cui la protezione potrebbe essere inefficace: quello in cui il file viene scaricato in un disco completamente vuoto, e viene quindi allocato a partire dal primo settore del disco e su settori contigui. Se il file viene copiato in un altro disco completamente vuoto, la protezione non è in grado di operare. Questo possibile problema, come pure quello della debolezza

della protezione in caso di mancanza di frammentazione, può essere risolto introducendo appositamente un certo grado di frammentazione al momento della scrittura del file. Questo può essere ottenuto sia accedendo a funzioni a basso livello del sistema operativo, sia (particolarmente nei sistemi FAT) chiudendo e riaprendo il file più volte durante la scrittura ed andando, tra una scrittura e l'altra, a scrivere un file fittizio, di dimensioni variabili, che, andando ad occupare i primi settori liberi del disco, crea una frammentazione nel file multimediale. Il file fittizio può essere aperto più volte, aggiungendo lunghezze variabili di dati, e cancellato alla fine della scrittura del file multimediale.

La dimensione dei "gap" di frammentazione è preferibilmente pseudocasuale e, perché non sia uguale per tutti i file multimediali, può usare come seme del numero casuale la chiave pubblica dell'utente o una sua parte; il grado di frammentazione così generato non deve essere necessariamente molto spinto, ma sufficiente a garantire il livello di protezione desiderato.

La descrizione finora riportata assume che la zona dati del file multimediale sia protetta con il metodo descritto nel brevetto 102015000056882; naturalmente, nei casi meno importanti, questa protezione non è indispensabile perché si possa utilizzare il metodo di protezione dalla copia.

Anche il formato dei dati, anziché quello con coda di dati previsto dal brevetto RM2013A000728, può essere quello tradizionale finora usato per il tipo di file multimediale desiderato.

Per evitare le conseguenze dovute a modifiche non autorizzate alla tabella di allocazione dei settori (che può avvenire dopo la decifrazione), vi si può aggiungere una hash di controllo (di tutto il file o di parte di esso) codificata con la chiave privata del cedente del file multimediale (firma digitale).

Se, nonostante la protezione, si dovessero trovare in circolazione delle copie del file multimediale fatte circolare assieme alla loro chiave di lettura (chiave privata dell'utente), è possibile dalla chiave risalire senza possibilità di

smentita all'autore della copia non autorizzata.

Il sistema ha un possibile punto debole: se si usa un programma di deframmentazione del disco, e questo deframmenta il file multimediale o comunque ne alloca una parte in una zona diversa del disco, il file diventa inutilizzabile. In alcuni sistemi operativi è possibile contrassegnare il file come "da non deframmentare", in modo da evitare questa possibilità. In altri sistemi, quali ad esempio Linux e derivati, la deframmentazione non è normalmente necessaria e i programmi di deframmentazione spesso non sono nemmeno installati. Un metodo per evitare la deframmentazione di un file è quello di farlo apparire come "aperto" o "in uso" nel momento in cui si avvia il programma di deframmentazione.

Quando il metodo descritto nel presente brevetto avrà una sufficiente diffusione, i produttori di programmi di deframmentazione certamente faranno in modo che le loro utility non deframmentino i file multimediali del tipo qui descritto.

È infine chiaro che all'oggetto della presente invenzione possono essere applicate aggiunte, modifiche o varianti ovvie per un tecnico del ramo senza per questo fuoriuscire dall'ambito di tutela fornito dalle rivendicazioni annesse.

Rivendicazioni

1. Metodo di protezione di file multimediali da copia e distribuzione non autorizzata, il detto metodo essendo caratterizzato dal fatto di comprendere:

   - un passo di creazione di un file multimediale (1002) in una memoria (1000), in cui il detto file multimediale (1002) presenta una pluralità di settori;

   - un passo di creazione su detto file multimediale (1002) di un settore (P) d'autorizzazione, in cui in detto settore (P) d'autorizzazione vengono memorizzati una pluralità di permessi di accesso e/o lettura del detto file multimediale (P);

   - un passo di creazione in detta memoria (1000) di una tavola di allocazione di una pluralità di settori di dati e comandi (1003) di detto file multimediale (1002);

   - un passo di crittazione del detto settore (P) d'autorizzazione e della detta tavola di allocazione di una pluralità di settori di dati e comandi (1003) di detto file multimediale, in cui la crittazione avviene con una prima chiave di crittazione pubblica.

2. Metodo secondo la rivendicazione 1, caratterizzato dal fatto che in un passo di scaricamento del detto file multimediale (1002), il detto file multimediale (1002) viene scaricato un settore per volta (2100) in un file di destinazione contenuto in una memoria di destinazione, ed in cui è presente un passo di lettura ripetuto per ogni settore scaricato, in cui un programma per elaboratore accede al sistema operativo o ad una tabella di allocazione dei file della detta memoria di destinazione, e carica (2200) un indirizzo fisico del settore appena scaricato.

3. Metodo secondo la rivendicazione 2, in cui in il detto programma per elaboratore, dopo aver acceduto al detto sistema operativo o alla detta tabella di allocazione di file, aggiunge una nuova riga (2300) ad una tabella di allocazione dei settori di dati e comandi (1003), e ripete i passi di

trasferimento (2100), di ricavo dell'indirizzo fisico (2200) e di scrittura di una nuova riga (2300) fino alla fine del detto file multimediale (1002).

4. Metodo secondo una qualsiasi delle precedenti rivendicazioni 2-3, caratterizzato dal fatto che il detto programma per elaboratore esegue una generazione di detto settore (P) d'autorizzazione ed esegue un passo di memorizzazione (2500) entro il detto settore (P) d'autorizzazione di permessi di utilizzo del file.
5. Metodo secondo la rivendicazione 4, caratterizzato dal fatto che il detto programma per elaboratore, al termine del detto passo di memorizzazione (2500) esegue un passo di codifica (2600) della tavola di allocazione dei settori di dati e comandi (1003) sul detto file di destinazione e chiude il detto file (2800).
6. Metodo secondo una qualsiasi delle precedenti rivendicazioni, caratterizzato dal fatto di comprendere un passo di riproduzione del detto file multimediale (1002) in cui si ha dapprima un passo di lettura della tavola di allocazione dei settori di dati e comandi (1003) e un successivo passo di decrittazione (3100) della detta tavola di allocazione dei settori di dati e comandi (1003) del detto file multimediale (1002).
7. Metodo secondo la rivendicazione 6, caratterizzato dal fatto che il detto passo di decrittazione avviene impiegando la detta prima chiave di crittazione pubblica.
8. Metodo secondo la rivendicazione 5 o la rivendicazione 6, caratterizzato dal fatto di comprendere inoltre un passo di decrittazione del detto settore (P) d'autorizzazione e un passo di caricamento di una pluralità di dati di autorizzazione contenuti nel detto settore (P) d'autorizzazione dopo la decrittazione.
9. Metodo secondo la rivendicazione 8, caratterizzato dal fatto che una riproduzione elettronica del detto file multimediale (1002) avviene solamente

allorquando i detti dati di autorizzazione comprendono un'autorizzazione alla detta riproduzione e l'allocazione fisica dei settori del file nell'unità di memoria coincide con quella scritta nella tavola di allocazione presente nel file stesso.

10. Metodo secondo la rivendicazione 8 o la rivendicazione 9, caratterizzato dal fatto di comprendere nella riproduzione del detto file multimediale (1002) una lettura sequenziale (3400) della pluralità di settori del detto file multimediale (1002) impiegando la detta tavola di allocazione dei settori di dati e comandi (1003) memorizzata nel file multimediale (1002) stesso.
11. Metodo secondo la rivendicazione 10, caratterizzato dal fatto di comprendere un passo di caricamento di almeno parte della detta pluralità di settori del detto file multimediale (1002) in uno stadio buffer di un dispositivo elettronico di riproduzione del detto file.
12. Metodo secondo la rivendicazione 11 o la rivendicazione 12, caratterizzato dal fatto che all'interno di almeno parte dei detti settori del detto file multimediale (1002) sono contenuti dati utili cifrati mediante codifica simmetrica con una chiave di scrambling.
13. Metodo secondo la rivendicazione 12, caratterizzato dal fatto che la detta chiave di scrambling è scritta nel detto file multimediale (1002) mediante codifica asimmetrica.
14. Metodo secondo la rivendicazione 12, caratterizzato dal fatto che la detta chiave di scrambling è una chiave ad uso singolo ottenuta da un sito internet predefinito.
15. Metodo secondo la rivendicazione 12, caratterizzato dal fatto che la detta chiave di scrambling è una chiave ad uso cablata all'interno di un programma per elaboratore di decodifica del detto file multimediale (1002).
16. Metodo secondo una qualsiasi delle precedenti rivendicazioni, caratterizzato dal fatto di comprendere un passo di copiatura del detto file multimediale

(1002) a sua volta comprendente un passo di decodifica (4100) della detta tavola di allocazione di settori di dati e comandi (1003) e del detto settore (P) d'autorizzazione del detto file multimediale (1003) ed un successivo passo di lettura (4400) da detta tavola di allocazione di settori di dati e comandi (1003) del detto file multimediale (1002) di un settore ed un passo di successiva scrittura (4500) del settore appena letto in un file di destinazione.

17. Metodo secondo la rivendicazione 16, caratterizzato dal fatto che a seguito del detto passo di successiva scrittura (4500) del settore appena letto in detto file di destinazione, il detto programma per elaboratore legge il numero fisico del settore del file di destinazione appena scritto e aggiunge una riga contenente tale numero fisico nella tavola di allocazione dei settori di dati e comandi (1003) del detto file di destinazione.
18. Programma per elaboratore elettronico, caricato su di un supporto di memoria non transitorio e atto ad essere eseguito su di un elaboratore elettronico, il detto programma essendo atto causare l'esecuzione di almeno parte dei passi descritti in una qualsiasi delle precedenti rivendicazioni 1-17.
19. File multimediale (1002) caratterizzato dal fatto di comprendere una struttura avente una pluralità di settori, in cui in detta pluralità di settori, almeno parte è atta a contenere dati utili multimediali ed in cui in detta pluralità di settori sono presenti:

    - almeno un settore (P) d'autorizzazione contenente dati elettronici di autorizzazione alla lettura o copiatura dei detti dati utili multimediali e/o del detto file multimediale stesso; e
    - una tavola di allocazione di settori di dati e comandi (1003) del detto file multimediale (1002), in cui la detta tavola di allocazione di settori di dati e comandi del detto file multimediale è crittata assieme al detto settore (P) d'autorizzazione.

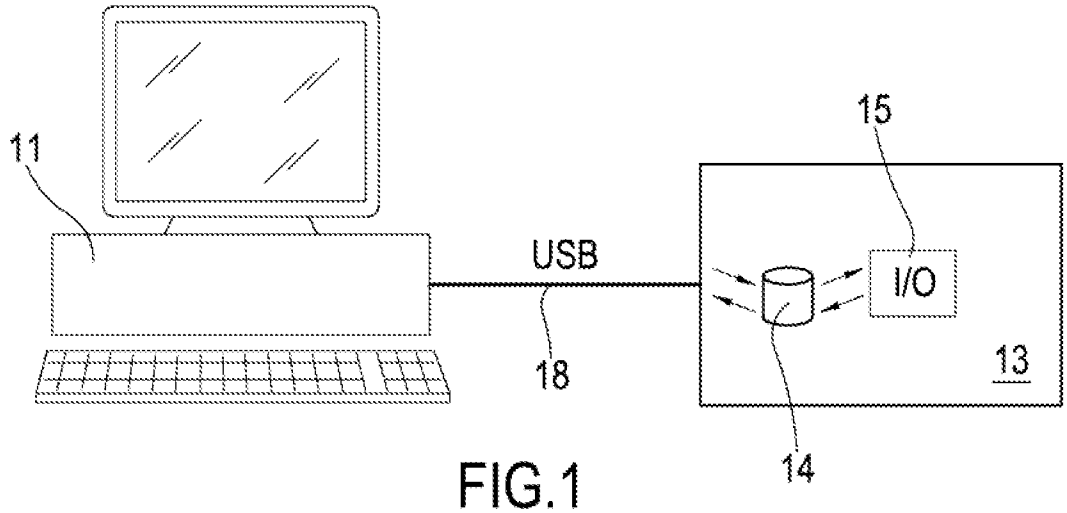


FIG.1

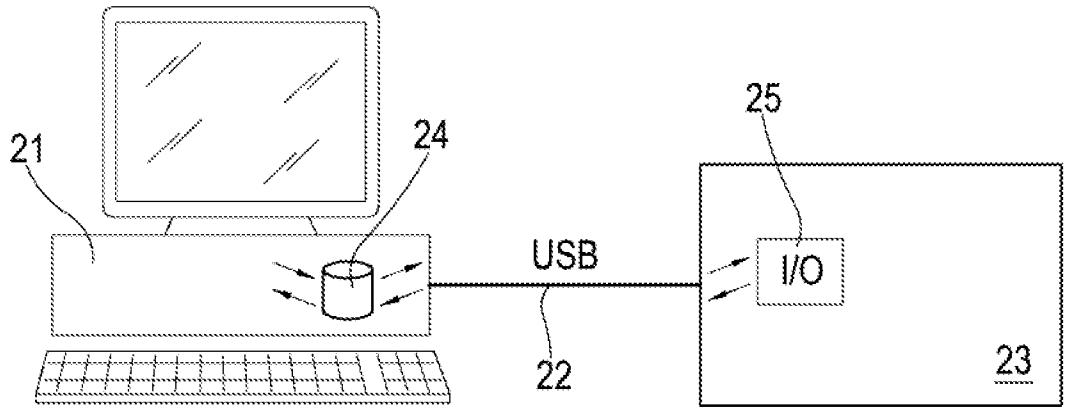


FIG.2

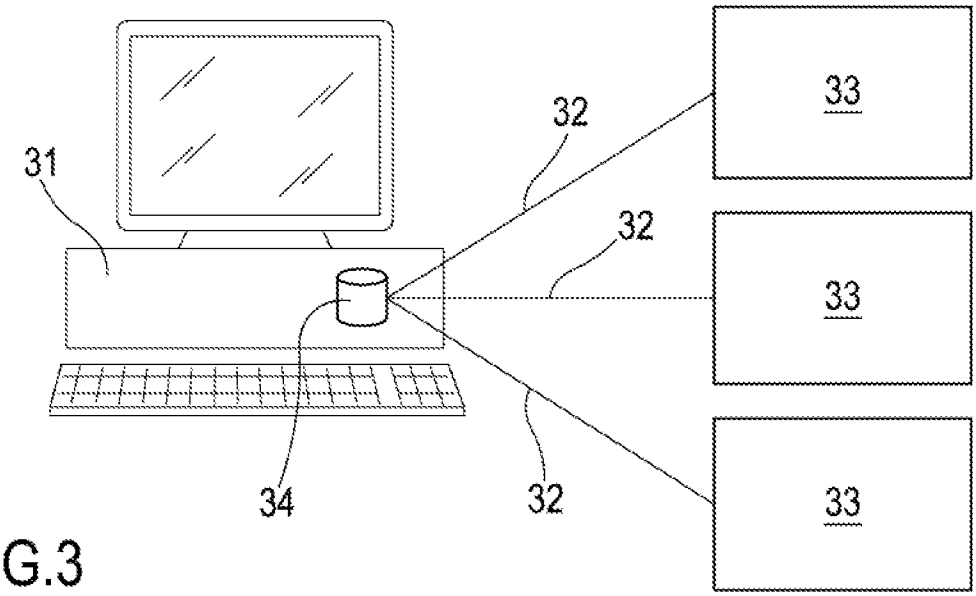


FIG.3

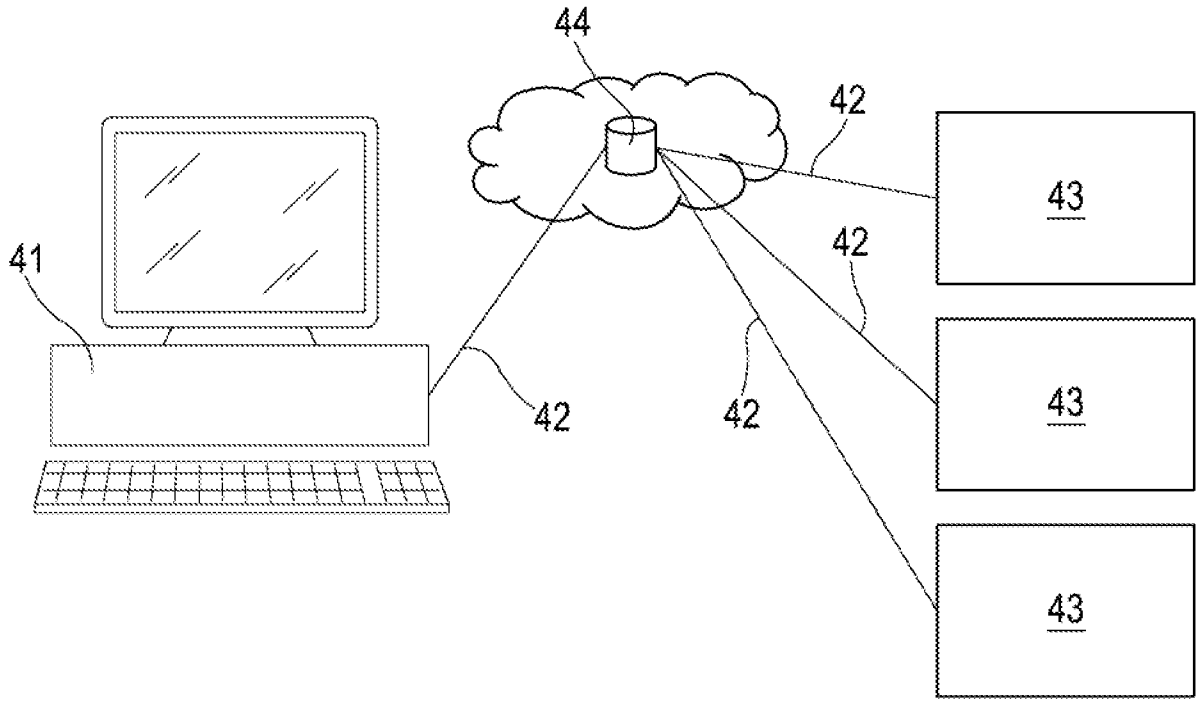


FIG.4

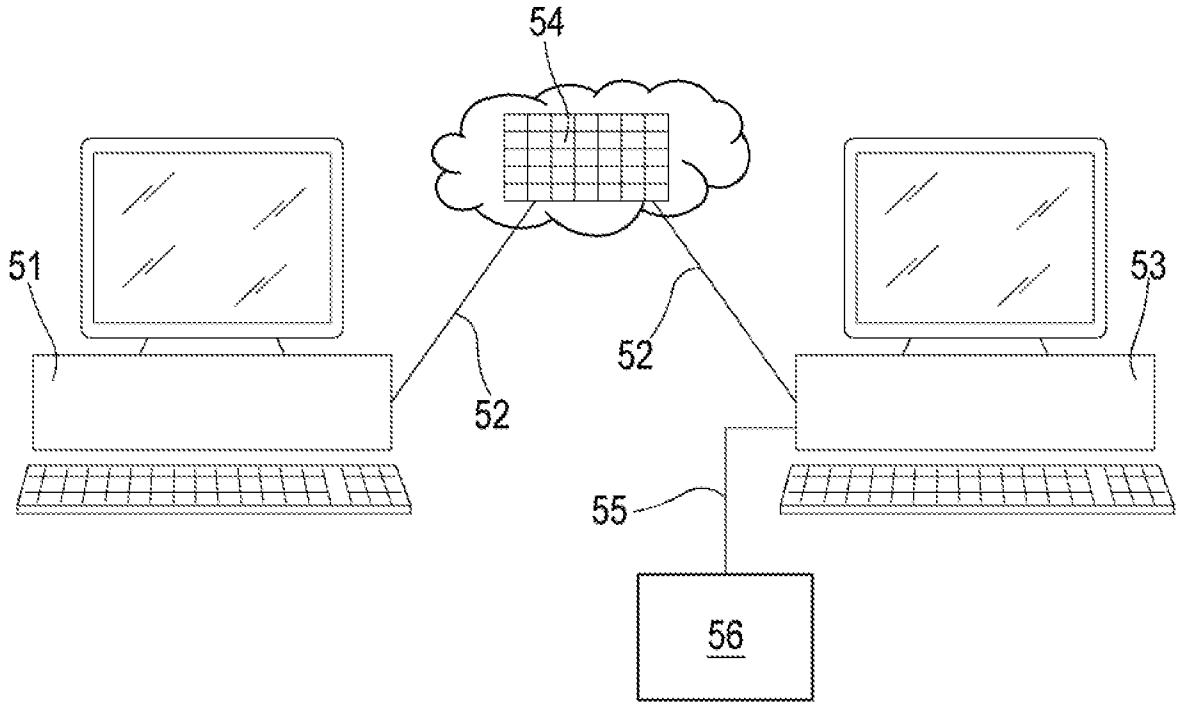


FIG.5

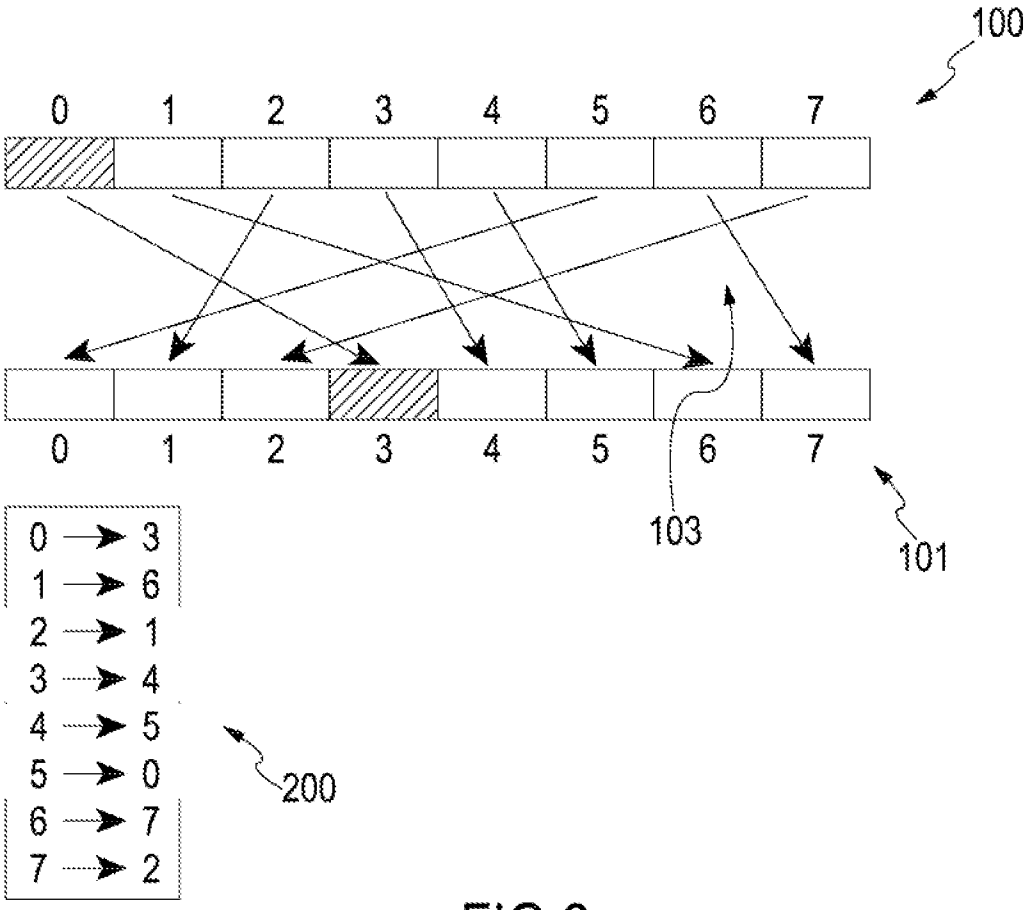

100
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7
103
101
0 → 3
1 → 6
2 → 1
3 → 4
4 → 5
5 → 0
6 → 7
7 → 2
200

FIG.6

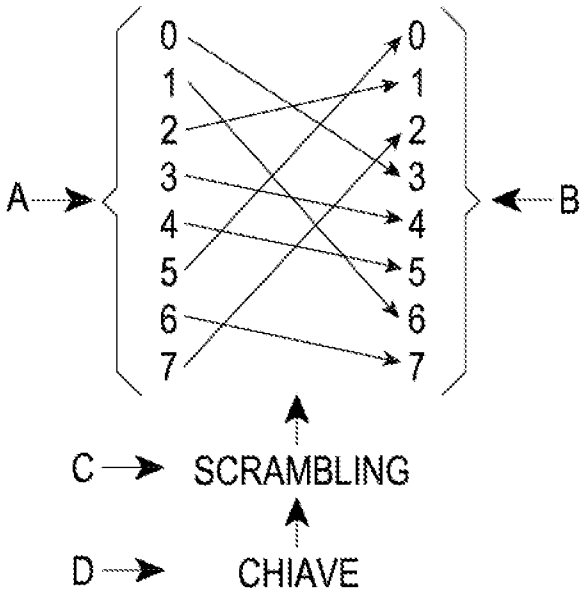

A
B
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7
C → SCRAMBLING
D → CHIAVE

FIG.7

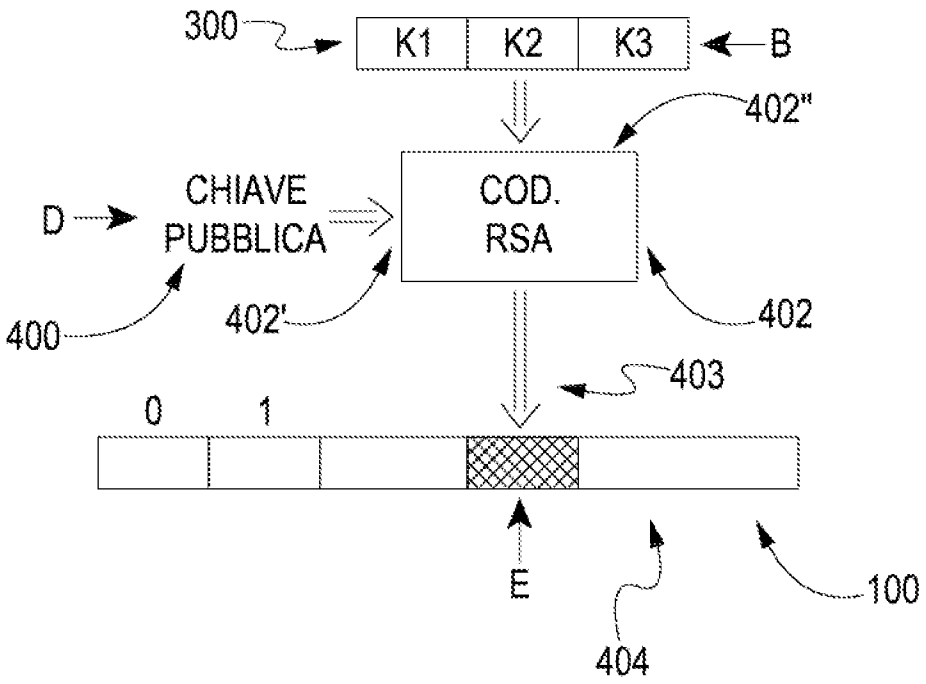

300
K1
K2
K3
B
402"
D
CHIAVE
PUBBLICA
COD.
RSA
400
402'
402
403
0
1
E
404
100

FIG.8

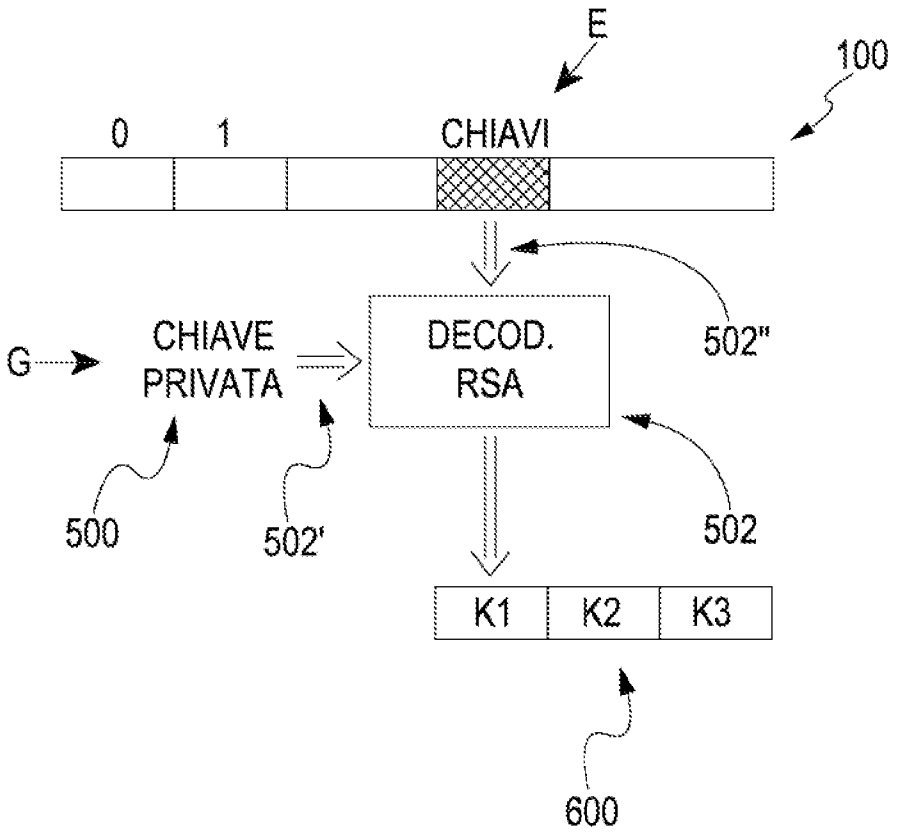

E
100
0
1
CHIAVI
G
CHIAVE
PRIVATA
DECOD.
RSA
502"
500
502'
502
K1
K2
K3
600

FIG.9

FIG.10

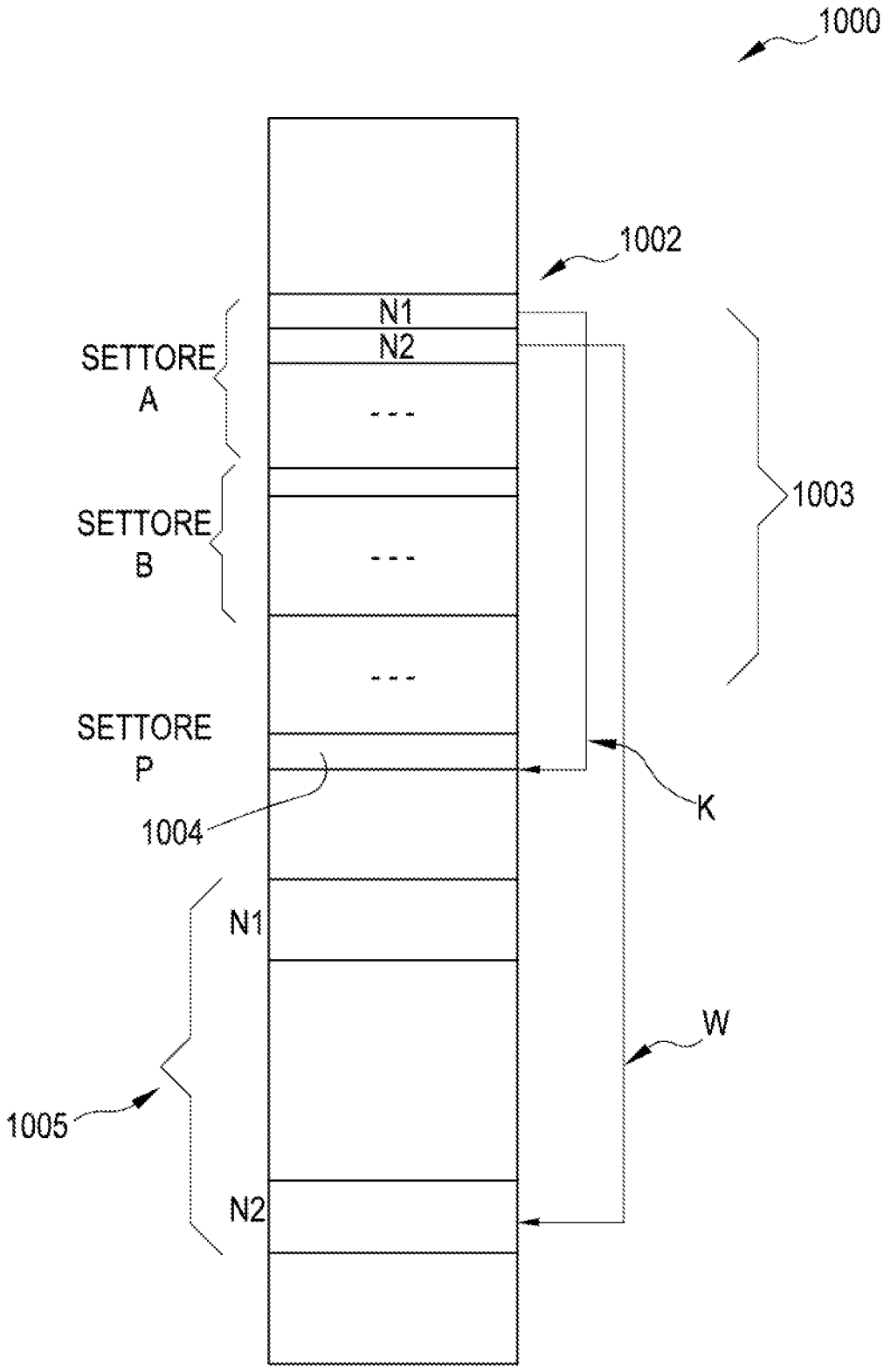
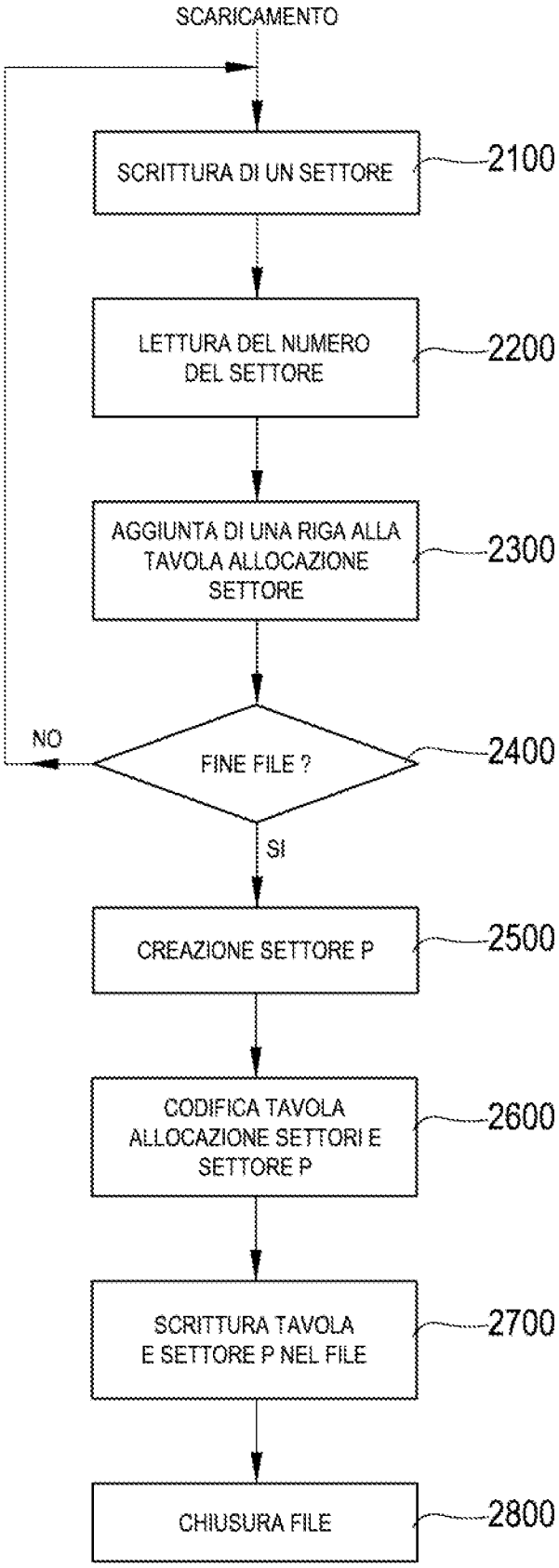

1000
1002
N1
N2
SETTORE A
- - -
SETTORE B
- - -
- - -
1003
SETTORE P
1004
K
N1
W
1005
N2

FIG.11


SCARICAMENTO
SCRITTURA DI UN SETTORE
2100
LETTURA DEL NUMERO DEL SETTORE
2200
AGGIUNTA DI UNA RIGA ALLA TAVOLA ALLOCAZIONE SETTORE
2300
NO
FINE FILE ?
2400
SI
CREAZIONE SETTORE P
2500
CODIFICA TAVOLA ALLOCAZIONE SETTORI E SETTORE P
2600
SCRITTURA TAVOLA E SETTORE P NEL FILE
2700
CHIUSURA FILE
2800

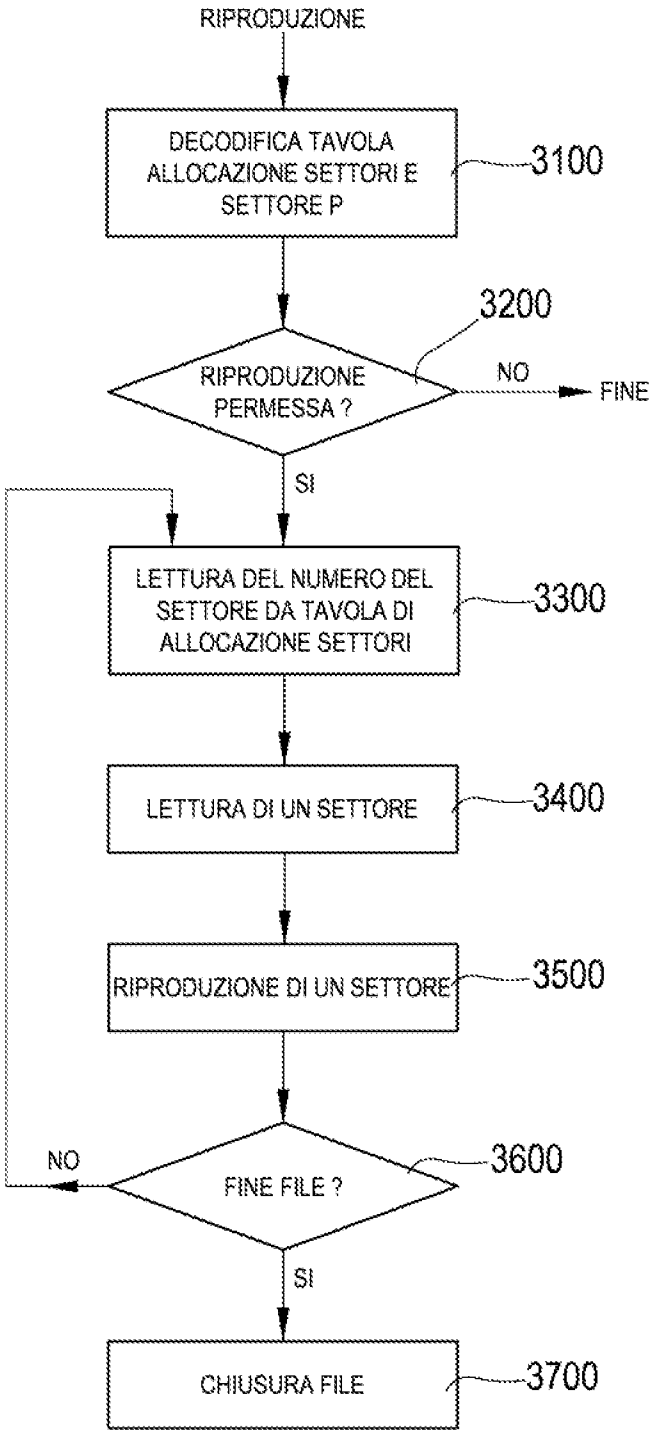

RIPRODUZIONE
DECODIFICA TAVOLA ALLOCAZIONE SETTORI E SETTORE P
3100
3200
RIPRODUZIONE PERMESSA ?
NO
FINE
SI
LETTURA DEL NUMERO DEL SETTORE DA TAVOLA DI ALLOCAZIONE SETTORI
3300
LETTURA DI UN SETTORE
3400
RIPRODUZIONE DI UN SETTORE
3500
NO
FINE FILE ?
3600
SI
CHIUSURA FILE
3700

FIG.12

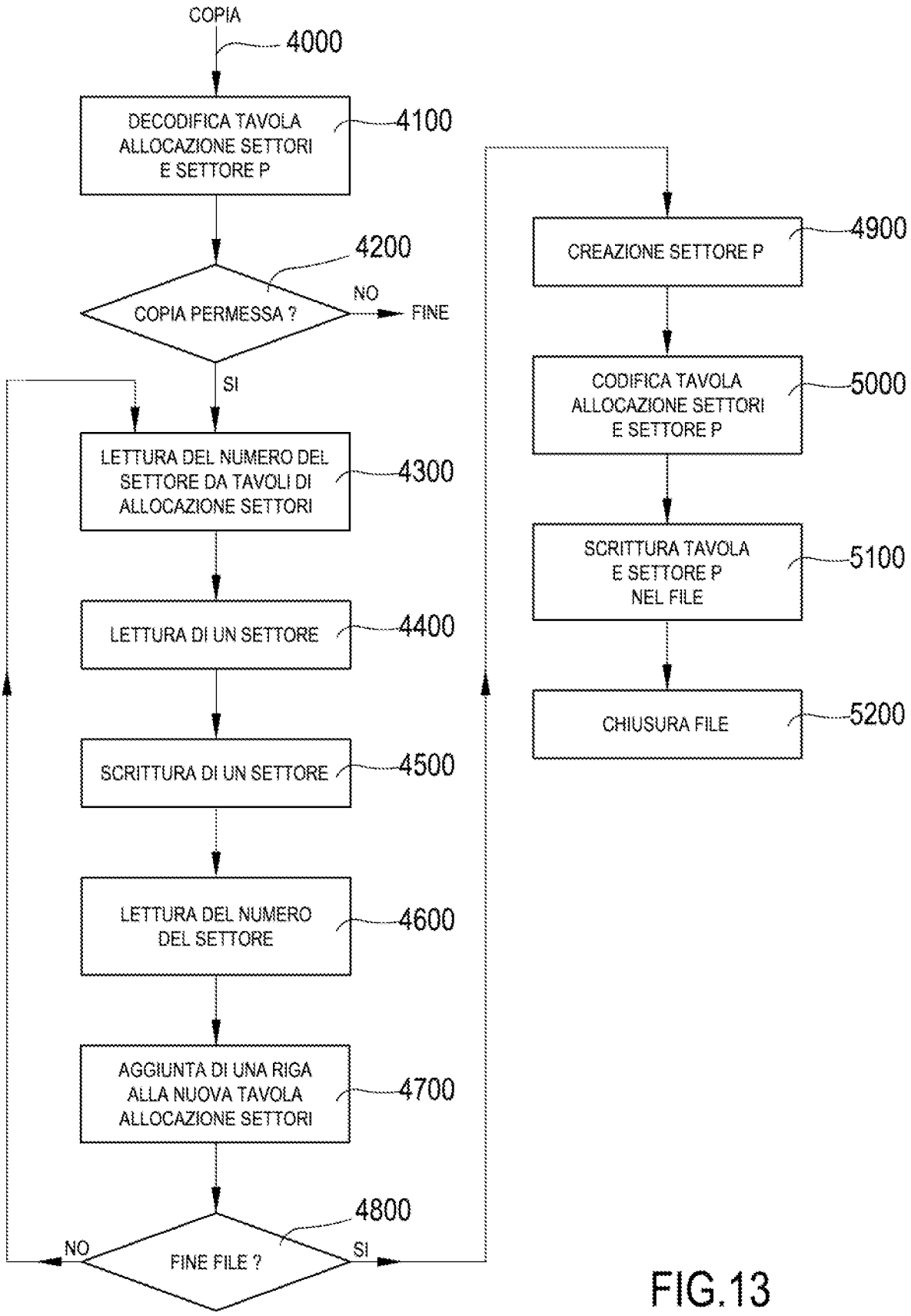

COPIA
4000
DECODIFICA TAVOLA ALLOCAZIONE SETTORI E SETTORE P
4100
4200
COPIA PERMESSA ?
NO
FINE
SI
LETTURA DEL NUMERO DEL SETTORE DA TAVOLI DI ALLOCAZIONE SETTORI
4300
LETTURA DI UN SETTORE
4400
SCRITTURA DI UN SETTORE
4500
LETTURA DEL NUMERO DEL SETTORE
4600
AGGIUNTA DI UNA RIGA ALLA NUOVA TAVOLA ALLOCAZIONE SETTORI
4700
4800
FINE FILE ?
NO
SI
CREAZIONE SETTORE P
4900
CODIFICA TAVOLA ALLOCAZIONE SETTORI E SETTORE P
5000
SCRITTURA TAVOLA E SETTORE P NEL FILE
5100
CHIUSURA FILE
5200

FIG.13